J. Symbolic Computation (1985) **1**, 271–281

Symbolic Iterative Algorithm for Generalised Inversion of Rational Polynomial Matrices

E. V. KRISHNAMURTHY

Department of Computer Science, University of Waikato, Hamilton, New Zealand

(*Received* 22 *August* 1984)

A symbolic iterative algorithm, based on Hensel's lemma and the Newton–Schultz method, is described for the generalised inversion of rational polynomial matrices over a field. The approach presented here unifies the computational framework for the inversion of both the numerical and polynomial matrices and provides the possibility for parallel implementation using array processors. This algorithm requires $0(m^3 4^{\log R})$ polynomial multiplications over a field, where m is the order of the matrix and the R the maximal degree of the rational polynomial element in the generalised inverse.

1. Introduction

Hensel's p-adic analysis plays a central role in mathematical research, serving as a bridge between the classical analysis and algebra (Koblitz, 1977). The beauty and expediency of the approach based on Hensel fields (p-adic and formal power series fields) for exact numerical (Gregory & Krishnamurthy, 1984) and symbolic computations (Krishnamurthy, 1985) in linear algebra is now well understood (see also Miola & Yun, 1974; Musser, 1975; Yun, 1976; Wang, 1978).

This paper describes a symbolic recursive (or iterative) algorithm for the inversion and generalised inversion of matrices whose elements are single or multivariable rational polynomials over a field. This algorithm is based on Zassenhaus–Hensel lemma (Zassenhaus, 1969) an important theorem in Hensel fields. Due to the limitations of space, we will confine ourselves to essential details; for background material and fuller details reference is made to the book on polynomial matrix computations (Krishnamurthy, 1985).

2. Generalised Inverses

If a matrix is rectangular or if a square matrix is singular, it does not have an inverse in the usual sense, but under certain conditions there exists, a generalised inverse (called g-inverse) (Rao & Mitra, 1971; Bhaskara Rao, 1981; 1983; Gregory & Krishnamurthy, 1984; Krishnamurthy, 1985). Let $\mathbf{A}$ be an $m \times n$ matrix over a field F and $\mathbf{G}$ an $n \times m$ matrix; consider the matrix equations:

(a) $\mathbf{AGA} = \mathbf{A}$
(b) $\mathbf{GAG} = \mathbf{G}$
(c) $(\mathbf{AG})^T = \mathbf{AG}$
(d) $(\mathbf{GA})^T = \mathbf{GA}$.

0747-7171/85/030271+11 $03.00/0

The matrix **G** is called:

(i) a g-inverse of **A**, denoted by $\mathbf{A}^-$ if (a) holds
(ii) a reflexive g-inverse of **A**, denoted by $\mathbf{A}_R^-$ if both (a) and (b) hold
(iii) a least squares g-inverse of **A**, denoted by $\mathbf{A}_L^-$ if both (a) and (c) hold
(iv) a minimum norm g-inverse of **A** denoted by $\mathbf{A}_M^-$ if both (a) and (d) hold,
and
(v) the Moore–Penrose inverse of **A**, denoted by $\mathbf{A}^+$, if (a), (b), (c) and (d) all hold.

Note that when **A** is a square non-singular matrix, a g-inverse reduces to the ordinary inverse $\mathbf{A}^{-1}$.

To compute a generalised inverse over F we can use the direct method described in Gregory & Krishnamurthy (1984):

Step 1: Obtain $\mathbf{M} = (\mathbf{A}\mathbf{A}^T)^2$ and find its reflexive inverse $\mathbf{M}_R^-$ using elementary row (column) operations:

$$E\mathbf{M} = \mathbf{M}_1$$

$$F\mathbf{M}_1^T = R = \begin{bmatrix} \mathbf{I}_r & 0 \\ 0 & 0 \end{bmatrix},$$

$\mathbf{I}_r$ is the identity matrix of size $r \times r$, where r is the rank of M.

(E and F are products of elementary matrices over $\bar{F}$.)

Step 2:

$$\mathbf{M}_R^- = F^T R E.$$

We then obtain $\mathbf{A}^+$, the Moore–Penrose inverse of **A**, using

$$\mathbf{A}^+ = \mathbf{A}^T \mathbf{M}_R^- (\mathbf{A}\mathbf{A}^T).$$

For rational polynomial matrices over a field the above definitions can be generalised and we can compute the various g-inverses. In this paper we describe a symbolic iterative method based on Hensel's lemma and Newton's method.

3. Hensel–Newton–Schultz Algorithm

Let $\mathbf{M}(x)$ be an $(m \times m)$ matrix over $F_p(x)$ [$F_p(x)$ denotes rational polynomials over the field $(\mathbf{I}_p, +, .)$ of integers modulo a prime p]. Let us assume that the denominators of the entries of $\mathbf{M}(x)$ are unity to begin with. Also let $\mathbf{M}_R^- = ((\mu_{ij}))$ denote the reflexive g-inverse of **M**. We will further assume that μ_{ij} belongs to $P(R-1/R-1, F_p(x))$, the set of Padé rational polynomials whose numerator and denominator degrees are $\leqslant (R-1)$. Further, let k be an integer such that

$$2^k \geqslant 2R-1.$$

Then, the following algorithm computes $\mathbf{M}_R^-$ provided, $\mathbf{M} \bmod x$ which is a matrix over $\mathbf{I}_p$, is not a zero matrix. (If $\mathbf{M} \bmod x = 0$, we can introduce a change of variable $y = x+a$).

ALGORITHM

Step 1. Construct $\mathbf{M} \bmod x$ which is a matrix over $\mathbf{I}_p$ and find

$$\mathbf{M}_R^- \bmod x = \mathbf{B}_1 \tag{1}$$

using the direct method described in Section 2. Thus

$$\mathbf{B}_1 = \mathbf{B}_1\mathbf{M}\mathbf{B}_1 \bmod x \tag{2}$$

and

$$\mathbf{M} = \mathbf{M}\mathbf{B}_1\mathbf{M} \bmod x \tag{3}$$

Step 2. For $i = 1, 2, \ldots, k$ compute the sequence

$$\mathbf{B}_{2^i} = \mathbf{B}_{2^{i-1}}(2I - \mathbf{M}\mathbf{B}_{2^{i-1}}) \bmod x^{2^i} \tag{4}$$

Step 3. At this point $\mathbf{M}_R^- = \mathbf{B}_{2^k}$; finally compute

$$\mathbf{A}^+ = \mathbf{A}^T\mathbf{M}_R^-(\mathbf{A}\mathbf{A}^T).$$

This algorithm rests on the following theorem.

THEOREM. *Let* $\mathbf{M}$ *be an* $(m \times m)$ *matrix over* $F_p(x)$ *and let* $\mathbf{M} \bmod x$ *possess a reflexive generalised inverse* $\mathbf{M}_R^- \bmod x$, *satisfying* $\mathbf{M}_R^-\mathbf{M}\mathbf{M}_R^- = \mathbf{M}_R^- \bmod x$ *and* $\mathbf{M}\mathbf{M}_R^-\mathbf{M} = \mathbf{M} \bmod x$. *Also let* $\mathbf{M}_R^- \bmod x = \mathbf{B}_1 = \mathbf{B}_{2^0}$. *Then the iteration*

$$\mathbf{B}_{2^i} = \mathbf{B}_{2^{i-1}}[2I - \mathbf{M}\mathbf{B}_{2^{i-1}}] \bmod x^{2^i}, \quad i \geqslant 1 \tag{5}$$

generates a polynomial matrix sequence $\{\mathbf{B}_{2^i}\}$, $i \geqslant 1$, *in* $\mathbf{I}_p[[x]]$ (*the infinite formal power series over* $\mathbf{I}_p$) *such that* $\mathbf{B}_{2^i}\mathbf{M}\mathbf{B}_{2^i} = \mathbf{B}_{2^i} \bmod x^{2^i}$ *and* $\mathbf{M}\mathbf{B}_{2^i}\mathbf{M} = \mathbf{M} \bmod x^{2^i}$.

PROOF. It is required to prove that when $\mathbf{M}_R^-$ exists at $2^k \geqslant 2R-1$, we can compute $\mathbf{M}_R^-$ using the iteration (5) and satisfying the properties:

$$\mathbf{M}\mathbf{B}_{2^i}\mathbf{M} \bmod x^{2^i} = \mathbf{M}$$

$$\mathbf{B}_{2^i}\mathbf{M}\mathbf{B}_{2^i} \bmod x^{2^i} = \mathbf{B}_{2^i} \quad \text{for } i = 1, 2, \ldots, k.$$

We prove this by induction:
For $i = 0$, this is true by construction:

$$\mathbf{M}\mathbf{B}_1\mathbf{M} \bmod x = \mathbf{M} \bmod x$$

$$\mathbf{B}_1\mathbf{M}\mathbf{B}_1 \bmod x = \mathbf{B}_1 \bmod x.$$

First, let us rewrite the equality:

$$\mathbf{M}\mathbf{B}_1\mathbf{M} = (\mathbf{M}\mathbf{B}_1)\mathbf{M} = [I + \mathbf{M}\mathbf{B}_1 - I]\mathbf{M} = \left[I + x\left[\frac{\mathbf{M}\mathbf{B}_1 - I}{x}\right]\right]\mathbf{M}$$

$$= [I + xK(x)]\mathbf{M} \tag{6}$$

where $K(x)$ is over $F_p(x)$ and similarly

$$\mathbf{B}_1\mathbf{M}\mathbf{B}_1 = \mathbf{B}_1(I + xR(x)) \tag{7}$$

or

$$\mathbf{B}_1\mathbf{M}\mathbf{B}_1 = (I + xS(x))\mathbf{B}_1 \tag{8}$$

where $R(x)$, $S(x)$ *are over* $F_p(x)$.

The equations (6), (7) and (8) suggest that we can write the inductive hypothesis for the step $(i-1)$ as:

$$\mathbf{MB}_{2^{i-1}}\mathbf{M} = [I + x^{2^{i-1}}K(x)]\mathbf{M} \tag{9}$$

$$\mathbf{B}_{2^{i-1}}\mathbf{MB}_{2^{i-1}} = \mathbf{B}_{2^{i-1}}[I + x^{2^{i-1}}R(x)] \tag{10}$$

$$\mathbf{B}_{2^{i-1}}\mathbf{MB}_{2^{i-1}} = [I + x^{2^{i-1}}S(x)]\mathbf{B}_{2^{i-1}} \tag{11}$$

to satisfy the requirements:

$$\mathbf{MB}_{2^{i-1}}\mathbf{M} \bmod x^{2^{i-1}} = \mathbf{M} \tag{12}$$

$$\mathbf{B}_{2^{i-1}}\mathbf{MB}_{2^{i-1}} \bmod x^{2^{i-1}} = \mathbf{B}_{2^{i-1}}. \tag{13}$$

Now to prove the theorem we assume the truth of (9), (10) and (11) at step $(i-1)$ and show that the iteration (5) results in the truth of (9), (10) and (11) for the succeeding step i.

We have by (5)

$$\mathbf{MB}_{2^i}\mathbf{M} = \mathbf{M}[\mathbf{B}_{2^{i-1}}(2I - \mathbf{MB}_{2^{i-1}})]\mathbf{M} = [2\mathbf{MB}_{2^{i-1}}\mathbf{M} - \mathbf{MB}_{2^{i-1}}\mathbf{MB}_{2^{i-1}}\mathbf{M}].$$

Using (9) this simplifies to

$$\begin{aligned}\mathbf{MB}_{2^i}\mathbf{M} &= [2(I + x^{2^{i-1}}K)\mathbf{M} - (I + x^{2^{i-1}}K)(I + x^{2^{i-1}}K)\mathbf{M}] \\ &= (I + x^{2^{i-1}}K)(2\mathbf{M} - \mathbf{M} - x^{2^{i-1}}K\mathbf{M}) \\ &= (I + x^{2^{i-1}}K)(I - x^{2^{i-1}}K)\mathbf{M} = (I - x^{2^i}K^2)\mathbf{M} = (I + x^{2^i}T)\mathbf{M},\end{aligned}$$

where $-K^2 = T$, as was to be proved.

Similarly by (5)

$$\begin{aligned}\mathbf{B}_{2^i}\mathbf{MB}_{2^i} &= \mathbf{B}_{2^{i-1}}[2I - \mathbf{MB}_{2^{i-1}}]\mathbf{MB}_{2^{i-1}}[2I - \mathbf{MB}_{2^{i-1}}] \\ &= [2\mathbf{B}_{2^{i-1}} - \mathbf{B}_{2^{i-1}}\mathbf{MB}_{2^{i-1}}]\mathbf{M}[2\mathbf{B}_{2^{i-1}} - \mathbf{B}_{2^{i-1}}\mathbf{MB}_{2^{i-1}}].\end{aligned}$$

Using (10) and (11) this simplifies to

$$\begin{aligned}&[2\mathbf{B}_{2^{i-1}} - \mathbf{B}_{2^{i-1}} - x^{2^{i-1}}S\mathbf{B}_{2^{i-1}}]\mathbf{M}[2\mathbf{B}_{2^{i-1}} - \mathbf{B}_{2^{i-1}} - x^{2^{i-1}}\mathbf{B}_{2^{i-1}}R] \\ &\qquad = [I - x^{2^{i-1}}S]\mathbf{B}_{2^{i-1}}[I + x^{2^{i-1}}R][I - x^{2^{i-1}}R].\end{aligned}$$

This reduces to

$$[I - x^{2^{i-1}}S]\mathbf{B}_{2^{i-1}}[I - x^{2^i}R^2] = [2I - (I + x^{2^{i-1}}S)]\mathbf{B}_{2^{i-1}}[I - x^{2^i}R^2]$$

which on using (11) gives

$$\begin{aligned}&[2\mathbf{B}_{2^{i-1}} - \mathbf{B}_{2^{i-1}}\mathbf{MB}_{2^{i-1}}][I - x^{2^i}R^2] \\ &\qquad = \mathbf{B}_{2^{i-1}}[2I - \mathbf{MB}_{2^{i-1}}][I - x^{2^i}R^2] = \mathbf{B}_{2^i}[I - x^{2^i}R^2] = \mathbf{B}_{2^i}[I + x^{2^i}V]\end{aligned}$$

where $V = -R^2$, as was to be proved.

REMARK. If the degree of the Padé rational is unknown, we can replace the count loop (*for* statement) in Step 2 by a *while* loop:

while Padé $\mathbf{B}_{2^{(i-1)}} \neq$ Padé $\mathbf{B}_{2^{(i-2)}}$ *do* $\mathbf{B}_{2^i} \leftarrow \mathbf{B}_{2^{i-1}}(2I - \mathbf{MB}_{2^{i-1}}) \bmod x^{2^i}$.

[Here Padé (**M**) denotes the converted rational values of all the matrix Hensel codes in **M** over $F_p(x)$.] This means that we continue our iterative step until the converted Padé rationals are equal (to ensure that the full power series representation is obtained).

4. Conversion to Padé rational

We now describe how to convert a truncated $(2R-1)$ degree formal power series representation $I_p[[x]]$ (Hensel code $H(p, 2R-1, \alpha(x))$ to a rational polynomial

$$\alpha(x) = a(x)/b(x) \in P(R-1/R-1, F_p(x)).$$

For proof of this algorithm, see Krishnamurthy (1985).

We use the seed matrix

$$\begin{bmatrix} x^{2R-1} & 0 \\ H(p, 2R-1, \alpha(x)) & 1 \end{bmatrix} = \begin{bmatrix} a_{-1} & b_{-1} \\ a_0 & b_0 \end{bmatrix}$$

and compute the sequence of pairs (a_i, b_i) thus:

for $i = 1, 2, \ldots$, compute

$$q_i = \text{quotient}\left[\frac{a_{i-2}}{a_{i-1}}\right]$$

$$a_i = a_{i-2} - q_i a_{i-1}$$

$$b_i = b_{i-2} - q_i b_{i-1}$$

until degree $a_i \leqslant R-1$ and degree $b_i \leqslant R-1$. Then the equivalent Padé rational is

$$\frac{a(x)}{b(x)} = \frac{a_i}{b_i}.$$

EXAMPLE. Convert $H(601, 5, \alpha(x)) = (1, 600, 2, 595, 24; 0)$. The computations are shown below. We stop at the second step as the degree conditions are met with $(R-1 = 2)$.

	x^5	0
	$24x^4+595x^3+2x^2+600x+1$	1
$-25x+144$	$313x^3-313x^2+169x-144$	$25x-144$
$50x-263$	$-16x^2-40x-8$	$-48x^2-48x-8$

Thus

$$\alpha(x) = \frac{-16x^2-40x-8}{-48x^2-48x-8} = \frac{2x^2+5x+1}{6x^2+6x+1} \in P(2/2, F_{601}(x))$$

5. Inversion of matrices in $Q(x)$

In order to extend the algorithm in Section 3 to matrices whose elements are polynomials over rational numbers $[Q(x)]$, we need to map the rational coefficients as described in Gregory & Krishnamurthy (1984) (see Example below) to a finite field

modulo p; the choice of p is governed by the coefficient and degree size in the g-inverse of the polynomial matrix.

If the elements of the g-inverse belong to the Padé rational polynomial $P(R-1/R-1, N, x)$ where N is the coefficient size in the denominator and numerator polynomials and $(R-1)$ the maximal numerator and denominator degrees, then:

$$p \geqslant 2RN^2+1.$$

The number of steps i of the algorithm is then given by

$$2^i \geqslant 2R-1.$$

The resulting matrix $\mathbf{B}_{2^i}$ is first mapped into $P(R-1/R-1, F_p(x))$ and then to $P(R-1/R-1, N, x)$ using the following Euclidean algorithm (Gregory & Krishnamurthy, 1984).

Start with the seed matrix

$$\begin{bmatrix} a_{-1} & b_{-1} \\ a_0 & b_0 \end{bmatrix} = \begin{bmatrix} p & 0 \\ \alpha & 1 \end{bmatrix}$$

where p is the prime chosen and α is any coefficient $\in I_p$ in the Padé rational polynomial $a(x)/b(x) \in F_p(x)$. Compute the sequence of pairs (a_i, b_i) thus:

for $i = 1, 2, \ldots$

$$q_i = \text{quotient}\left[\frac{a_{i-2}}{a_{i-1}}\right]$$

$$a_i = a_{i-2} - q_i a_{i-1}$$

$$b_i = b_{i-2} - q_i b_{i-1}$$

until $|a_i|, |b_i| \leqslant N$.

Then the equivalent rational to $\alpha = a_i/b_i$.

EXAMPLE. Convert $403 \in I_{601}$ into rational

$$N \leqslant \sqrt{\frac{601-1}{2 \cdot 3}} = 10.$$

We start with the seed matrix

$$\begin{bmatrix} 601 & 0 \\ 403 & 1 \end{bmatrix}$$

and obtain the following table:

	601	0
	403	1
1	198	−1
2	7	3
28	2	−85

Thus 403 maps to the rational 7/3.

6. Examples for Algorithms

(i) Let

$$\mathbf{M} = \begin{bmatrix} 1+x & 1+x \\ 1+x & 1+x \end{bmatrix} \in F_3(x); \quad \text{find } \mathbf{M}_R^-.$$

We choose $(2R-1) = 3$; $R-1 = 1$; thus $k \geqslant 2$ (or it is sufficient to iterate 2 times).

We have

$$\mathbf{M}_R^- \bmod x = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}_R^- = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \mathbf{B}_1.$$

We then obtain $\mathbf{B}_2 = \mathbf{B}_1[2I - \mathbf{M}\mathbf{B}_1] \bmod x^2$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\left[\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} - \begin{bmatrix} 1+x & 1+x \\ 1+x & 1+x \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\right] \bmod x^2 = \begin{bmatrix} 1-x & 0 \\ 0 & 0 \end{bmatrix}$$

$$\mathbf{B}_4 = \mathbf{B}_2[2I - \mathbf{M}\mathbf{B}_2] \bmod x^4$$

$$= \begin{bmatrix} 1-x & 0 \\ 0 & 0 \end{bmatrix}\left[\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} - \begin{bmatrix} 1+x & 1+x \\ 1+x & 1+x \end{bmatrix}\begin{bmatrix} 1-x & 0 \\ 0 & 0 \end{bmatrix}\right] \bmod x^4$$

$$= \begin{bmatrix} 1-x & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1+x^2 & 0 \\ -1+x^2 & 0 \end{bmatrix} = \begin{bmatrix} 1-x+x^2-x^3 & 0 \\ 0 & 0 \end{bmatrix}.$$

We stop the iteration here. The result on conversion to Padé rational polynomial is given by:

$$\mathbf{M}_R^- = \begin{bmatrix} 1/1+x & 0 \\ 0 & 0 \end{bmatrix}.$$

(ii) Let

$$\mathbf{A} = \begin{bmatrix} 3+x & 1+X \\ 2+x & 2+x \end{bmatrix} \quad \text{where } a_{ij} \in Q(x).$$

Let us assume $N \leqslant 4$ and $(R-1) = 1$ or $R = 2$. Thus we choose $p = 101 > 2 \cdot 2 \cdot 16$; we need to iterate i times such that

$$2^i \geqslant (2R-1) = 3 \quad \text{or } i = 2.$$

The iterations are as follows:

$$\mathbf{B}_1 = \begin{bmatrix} 3 & 1 \\ 2 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} 51 & 25 \\ -51 & 26 \end{bmatrix}$$

$$\mathbf{A}\mathbf{B}_1 = \begin{bmatrix} 3+x & 1+x \\ 2+x & 2+x \end{bmatrix}\begin{bmatrix} 51 & 25 \\ -51 & 26 \end{bmatrix} = \begin{bmatrix} 1 & 51x \\ 0 & 1+51x \end{bmatrix}$$

$$(2I - \mathbf{A}\mathbf{B}_1) = \begin{bmatrix} 1 & -51x \\ 0 & 1-51x \end{bmatrix}$$

$$\mathbf{B}_2 = \mathbf{B}_1(2I - \mathbf{A}\mathbf{B}_1) = \begin{bmatrix} 51 & 25+63x \\ -51 & 26+63x \end{bmatrix}$$

$$\mathbf{AB}_2 = \begin{bmatrix} 1 & 25x^2 \\ 0 & 1+25x^2 \end{bmatrix}$$

$$(2I - \mathbf{AB}_2) = \begin{bmatrix} 1 & -25x^2 \\ 0 & 1-25x^2 \end{bmatrix}$$

$$\mathbf{B}_{2^2} = \mathbf{B}_4 = \begin{bmatrix} 51 & (41x^3+19x^2+63x+25) \\ 50 & (41x^3+19x^2+63x+26) \end{bmatrix}$$

which in Hensel code form is

$$\mathbf{B}_4 = \begin{bmatrix} (51;0) & (25,63,19,41;0) \\ (50;0) & (26,63,19,41;0) \end{bmatrix}.$$

On conversion to $P(1/1, F_{101}(x))$ (section 4) $\mathbf{B}_4$ becomes

$$|\mathbf{A}^{-1}|_{101} = \begin{bmatrix} 51 & (25+25x)/(1+51x) \\ 50 & (26+76x)/(1+51x) \end{bmatrix}.$$

Each one of the coefficients in $|\mathbf{A}^{-1}|_{101}$ on conversion gives

$$\mathbf{A}^{-1} = \begin{bmatrix} 1/2 & \dfrac{-(1/4+1/4x)}{(1+1/2x)} \\ -1/2 & \dfrac{(3/4+1/4x)}{(1+1/2x)} \end{bmatrix}$$

$$= \begin{bmatrix} 1/2 & \dfrac{-(1+x)}{4+2x} \\ -1/2 & \dfrac{(3+x)}{4+2x} \end{bmatrix} \in P(1/1, 4, x).$$

REMARKS. (i) When the coefficient size N is large we can choose a set of s distinct primes $p_1, p_2, \ldots, p_s$ (or their powers $p_i^{r_i}$) such that

$$M = \prod_{i=1}^{s} p_i^{r_i} \geqslant 2N^2R+1.$$

The computation is carried out independently (and in parallel, if speed is needed) with each p_i. The resulting entries of $|\mathbf{A}^{-1}|_{p_i}$ are then combined using the Chinese remainder theorem (Gregory & Krishnamurthy, 1984) to obtain $|\mathbf{A}^{-1}|_M$; these would then be the Hensel codes $H(M, r, \alpha(x))$. Using the method of section 4 these are converted to numerator and denominator polynomials in $I_M[x]$. The coefficients in the numerator and denominator polynomials which belong to I_M are then converted to rationals.

Let

$$\mathbf{A} = \begin{bmatrix} 3+x & 1+x \\ 2+x & 2+x \end{bmatrix}$$

where $a_{ij} \in Q(x)$.

We now illustrate the use of three different primes 3, 5, 7. Here,

$$|\mathbf{A}|_3 = \begin{bmatrix} x & (1+x) \\ (2+x) & (2+x) \end{bmatrix}; \quad |\mathbf{A}^{-1}|_3 = \begin{bmatrix} (2;\,0) & (2,\,1,\,1,\,1;\,0) \\ (1;\,0) & (0,\,1,\,1,\,1;\,0) \end{bmatrix}$$

$$|\mathbf{A}|_5 = \begin{bmatrix} (3+x) & (1+x) \\ (2+x) & (2+x) \end{bmatrix}; \quad |\mathbf{A}^{-1}|_5 = \begin{bmatrix} (3;\,0) & (1,\,3,\,1,\,2;\,0) \\ (2;\,0) & (2,\,3,\,1,\,2;\,0) \end{bmatrix}$$

$$|\mathbf{A}|_7 = \begin{bmatrix} (3+x) & (1+x) \\ (2+x) & (2+x) \end{bmatrix}; \quad |\mathbf{A}^{-1}|_7 = \begin{bmatrix} (4;\,0) & (5,\,6,\,4,\,5;\,0) \\ (3;\,0) & (6,\,6,\,4,\,5;\,0) \end{bmatrix}.$$

Using Chinese remainder theorem and combining, we obtain:

$$|\mathbf{A}^{-1}|_{105} = \begin{bmatrix} (53;\,0) & (26,\,13,\,46,\,82;\,0) \\ (52;\,0) & (27,\,13,\,46,\,82;\,0) \end{bmatrix}$$

which on conversion to $P(1/1, F_{105}(x))$ results in

$$|\mathbf{A}^{-1}|_{105} = \begin{bmatrix} 53 & (26+26x)/(1+53x) \\ 52 & (27+79x)/(1+53x) \end{bmatrix}.$$

The coefficients of the entries in $|\mathbf{A}^{-1}|_{105}$ are now converted to rationals using the Euclidean algorithm. Thus

$$\mathbf{A}^{-1} = \begin{bmatrix} 1/2 & \dfrac{-(1/4+1/4x)}{(1+1/2x)} \\ -1/2 & \dfrac{(3/4+1/4x)}{(1+1/2x)} \end{bmatrix}.$$

7. Extension to Multivariable Polynomial Matrices

The algorithm described in section 3 can be extended to invert (or g-invert) a multivariable matrix polynomial. The resulting formal power series representation of the rational polynomials (Hensel Codes (Krishnamurthy, 1985)) can be converted to Padé rational polynomials by using Toeplitz matrix method (Chisholm, 1977; Baker & Graves-Morris, 1981).

Let $\mathbf{A} = a_{ij}(x_1, \ldots, x_n)$ be an $(m \times m)$ matrix whose elements are n variable rational polynomial functions over I_p. Let us assume that the reflexive inverse $\mathbf{A}_R^-$ exists and its elements belong to $P(R-1, \ldots, R-1/R-1, \ldots, R-1, F_p(x_1, x_2, \ldots, x_n))$. We also define the notion of ord thus; let $\mathbf{M}$ by any n-variable rational polynomial matrix over I_p; then $\mathbf{M}$ ord (k) denotes the matrix derived from $\mathbf{M}$ by retaining only those terms $x_1^{\beta_1} \ldots x_n^{\beta_n}$ for which

$$\beta_1 + \beta_2 + \ldots + \beta_n \leqslant k-1.$$

In the Hensel–Newton method we first construct

$$\mathbf{A}_R^- \text{ Ord } (1) = \mathbf{B}_1;$$

it is assumed $\mathbf{A}_R^-$ Ord (1) exists and satisfies

$$\mathbf{A}\mathbf{A}_R^-\mathbf{A} \text{ Ord } (1) = \mathbf{A}$$

$$\mathbf{A}_R^-\mathbf{A}\mathbf{A}_R^- \text{ Ord } (1) = \mathbf{A}_R^-.$$

We then use the iteration

$$\mathbf{B}_{2^i} = \mathbf{B}_{2^{i-1}}[2I - \mathbf{A}\mathbf{B}_{2^{i-1}}] \text{ Ord } (2^i),$$

for $i = 1, 2, \ldots, k$, where k is determined by the maximal degree of the elements of $\mathbf{A}_R^-$.

Here we need to iterate i times such that $2^i \geqslant 2n(R-1)+1$ to reconstruct the Padé rational polynomial belonging to

$$P(R-1, \ldots R-1/R-1, \ldots, R-1, F_p(x_1, \ldots, x_n))$$

uniquely.

The above procedure can be extended to rational polynomials over Q in the usual manner described earlier, by choosing a proper prime p or a product of power of primes that would be adequate to represent uniquely all the elements of $\mathbf{A}_R^-$.

EXAMPLE. Let

$$\mathbf{A} = \begin{bmatrix} 1+x+y & 1+x+y \\ 1+x+y & 1+x+y \end{bmatrix} \in F_7(x, y)$$

$$\mathbf{A}_R^- \text{ Ord } 1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \mathbf{B}_1.$$

Thus

$$\mathbf{B}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\left[\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} - \begin{bmatrix} 1+x+y & 1+x+y \\ 1+x+y & 1+x+y \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\right]$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1-x-y & 0 \\ -1-x-y & 2 \end{bmatrix} = \begin{bmatrix} 1-x-y & 0 \\ 0 & 0 \end{bmatrix}$$

$$\mathbf{B}_4 = \begin{bmatrix} 1-x-y & 0 \\ 0 & 0 \end{bmatrix}\left[\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} - \begin{bmatrix} 1-(x+y)^2 & 0 \\ 1-(x+y)^2 & 0 \end{bmatrix}\right]$$

$$= \begin{bmatrix} 1-x-y & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1+(x+y)^2 & 0 \\ -1+(x+y)^2 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 1-x-y+x^2+y^2+2xy-3x^2y-3xy^2-x^3-y^3 & 0 \\ 0 & 0 \end{bmatrix}.$$

This on conversion to Padé rational gives

$$\mathbf{A}_R^- = \frac{1}{1+x+y}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

REMARK. The above algorithm is quadratically convergent. One can use higher order convergent schemes as described in Krishnamurthy (1985).

8. Complexity Considerations

The method described here uses direct polynomial matrix multiplications. The earlier methods (McClellan, 1973, 1977; Krishnamurthy, 1985) use an evaluation–interpolation scheme which involve very high precision operands and require a very large number of numerical matrix inversions. The present method requires $0(4^k m^3)$ polynomial

multiplications where $2^k \geqslant 2R-1$. The final conversion from Hensel Code to Padé rationals (Brent *et al.*, 1980; Krishnamurthy, 1985) requires $0(m^2R\log^2 R)$. Thus the order of complexity is $0(m^3 4^{\log R})$.

References

Baker, G. A., Graves-Morris, P. (1981). Padé Approximants, Parts I and II. *Encyclopaedia of Mathematics*, Vols. 13 and 14. Reading, Mass: Addison-Wesley.

Bhaskara Rao, K. P. S. (1981). On generalized inverse of matrices over principal ideal rings. *Lin. Multilin. Alg.* **10**, 145–154.

Bhaskara Rao, K. P. S. (1983). On generalized inverses over integral domains. *Lin. Alg. Apps* **49**, 179–189.

Brent, R. P., Gustavson, F. G., Yun, D. Y. (1980). Fast solution of Toeplitz systems of equations and computation of Padé approximants. *J. Algor.* **1**, 259–295.

Chisholm, J. S. R. (1977). N-variable rational approximation. In: (Saff, E. B., Varga, R. S. eds) *Padé and rational approximation—theory and applications*. New York: Academic Press.

Gregory, R. T., Krishnamurthy, E. V. (1984). *Methods and applications of error-free computation*. New York: Springer-Verlag.

Koblitz, N. (1977). *p-adic numbers, p-adic analysis, and zeta functions*. New York: Springer-Verlag.

Krishnamurthy, E. V. (1985). *Error-free polynomial matrix computations*. New York: Springer-Verlag.

McClellan, M. T. (1973). The exact solution of linear equations with polynomial coefficients. *J. Assoc. Comp. Mach.* **20**, 563–588.

McClellan, M. T. (1977). The exact solution of linear equations with rational function coefficients. *ACM TOMS*, **3**, 1–25.

Miola, A., Yun, D. Y. (1974). The computational aspects of Hensel type univariable polynomial gcd algorithms. *Proc. EUROSAM 74*. pp. 46–54. Stockholm.

Musser, D. R. (1975). Multivariate polynomial factorization. *J. Assoc. Comp. Mach.* **22**, 291–308.

Rao, C. R., Mitra, S. K. (1971). *Generalized inverse of matrices and its applications*. New York: Wiley.

Wang, P. S. (1978). An improved multivariate polynomial factoring algorithms. *Math. Comp.* **32**, 1215–1231.

Yun, D. Y. Y. (1976). On square-free decomposition algorithms. *Proc. 1976 ACM SYMSAC*. pp. 26–35. Yorktown Heights, New York.

Zassenhaus, H. (1969). On Hensel factorization. *J. Number Theor.* **1**, 291–311.